Parallelization of Restricted Quantum Circuits using Ancillae (Algebraic Systems, Formal Languages and Computations)

AUTHOR(S):

Abe, Hideaki; Sung, Shao Chin

CITATION:

Abe, Hideaki ...[et al]. Parallelization of Restricted Quantum Circuits using Ancillae (Algebraic Systems, Formal Languages and Computations). 数理解析研究所講究録 2000, 1166: 1-7

ISSUE DATE:

2000-08

URL:

http://hdl.handle.net/2433/64362

数理解析研究所講究録
1166 巻 2000 年 1-7

Parallelization of Restricted Quantum Circuits using Ancillae

Hideaki Abe (安倍 秀明) Shao Chin Sung (宋 少秋)

School of Information Science
Japan Advanced Institute of Science and Technology
1-1 Asahidai, Tatsunokuchi, Ishikawa, 923-1292, Japan.
Email : {h_abe, son}@jaist.ac.jp

1 Introduction

Quantum circuits are proposed as a parallel model of quantum computation by Deutsch [3], in which computing devices, called *quantum gates*, are connected acyclicly. Here we are concerned with parallelization of quantum circuits by using ancillae (i.e., auxiliary quantum bits). By parallelization of quantum circuits, we mean to reduce depth of quantum circuits. In this paper, parallelizations of two types of quantum circuits are considered. The two types are quantum circuits consisting of controlled-not gates and phase-shift gates and quantum circuits consisting of controlled-not gates and Walsh-Hadamard gates. As a by-product, upper bounds of the number of ancillae for parallelizing such quantum circuits with n-input to logarithmic depth are reduced to $1/\log n$ of the upper bounds shown by Moore and Nilsson [4].

2 Preliminaries

Let us introduce some terminologies of quantum circuits (see [3, 5] for details). Let

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

For $x = (x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ with $n \geq 1$, let

$$|x\rangle = |x_1, x_2, \ldots, x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle,$$

where $\otimes$ is the tensor product operation. It follows that $|x\rangle$ is a unit vector of length 2^n for each $x \in \{0,1\}^n$. A matrix U is called *unitary* if $UU^\dagger = U^\dagger U = I$, where $U^\dagger$ is the transposed conjugate of U, and I is a unit matrix.

In quantum computation, a bit is represented by a two-state physical system, and is called a *qubit*. For $n \geq 1$, a state $|\psi\rangle$ of n-qubit can be represented as a superposition of $|x\rangle$s with $x \in \{0,1\}^n$,

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} a_x|x\rangle,$$

where all a_xs are complex numbers satisfying $\sum_{x\in\{0,1\}^n} |a_x|^2 = 1$. Each a_x is called the *amplitude* of $|x\rangle$ in $|\psi\rangle$, and for $a_x = |a_x|e^{ib_x}$, b_x is called the *phase* of $|x\rangle$ in state $|\psi\rangle$.

A *quantum circuit* is a directed networks connecting quantum gates acyclicly. Each quantum gate has the same number of inputs and outputs, and is specified by a unitary matrix in such a way that an k-input k-output *quantum gate* G for some $k \geq 1$, which is specified by a $2^k \times 2^k$ unitary matrix $U_{\mathrm{G}} = [u_{xy}]$ for $x, y \in \{0,1\}^k$, realizes a mapping of states of its inputs to states of its outputs as follows:

$$|x\rangle \mapsto \sum_{y\in\{0,1\}^k} u_{xy}|y\rangle.$$

Depth of a quantum circuit is the length (i.e., number of quantum gates) of the longest directed path in it. *Ancilla* is a qubit which is in state $|0\rangle$ at the beginning and the end of realization. We say that for some $\gamma \geq 0$, a quantum circuit with γ ancillae *realizes* a mapping

$$|x_1, x_2, \ldots, x_n\rangle \mapsto |y_1, y_2, \ldots, y_n\rangle,$$

if it realizes the mapping

$$|x_1, x_2, \ldots, x_n, 0^\gamma\rangle \mapsto |y_1, y_2, \ldots, y_n, 0^\gamma\rangle.$$

In this paper, we are concerned with the relation of depth and number of ancillae of quantum circuits.

Here We consider quantum circuits with *phase-shift gates*, *Walsh-Hadamard gates*, and *controlled-not gates*, and these gates are respectively specified by uni-

tary matrices PS_θ for $\theta : \{0,1\} \to [0, 2\pi)$, WH, and CN, which are defined as follows:

$$\mathrm{PS}_\theta = \begin{pmatrix} e^{i\theta(0)} & 0 \\ 0 & e^{i\theta(1)} \end{pmatrix}, \quad \mathrm{WH} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \mathrm{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

By applying PS_θ gate and WH gate to the j-th qubit of n-qubit, the mappings

$$\begin{aligned} |x_1, x_2, \ldots, x_n\rangle &\mapsto e^{i\theta(x_j)} |x_1, x_2, \ldots, x_n\rangle, \\ |x_1, x_2, \ldots, x_n\rangle &\mapsto \frac{1}{\sqrt{2}} \sum_{y \in \{0,1\}} (-1)^{y x_j} |x_1, \ldots, x_{j-1}, y, x_{j+1}, \ldots, x_n\rangle \end{aligned}$$

are realized, respectively. By applying CN gate to j-th qubit and k-th qubit of n-qubit respectively as its first and second input, the mapping

$$|x_1, x_2, \ldots, x_n\rangle \mapsto |x_1, \ldots, x_{k-1}, x_k \oplus x_j, x_{k+1}, \ldots, x_n\rangle$$

is realized. The first input of CN gate is called the *control-bit*, and the second input of CN gate is called the *target-bit*

For quantum circuits consisting of CN gates, following result was showed in [1].

Proposition 1 *Quantum circuits consisting of* CN *gates can be parallelized to*

$$O(n^2/\gamma + \log(\gamma/n))$$

depth by using γ ancillae for $\gamma \geq n$.

Let $\mathrm{CN}(n, m)$ be a set of mappings over states of $(n+m)$-qubit such that each mapping of $\mathrm{CN}(n, m)$ can be specified by an $n \times m$ 0-1 matrix $A = [a_{jk}]$ such that

$$|x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m\rangle \mapsto |x_1, x_2, \ldots, x_n, z_1, z_2, \ldots, z_m\rangle,$$

where $z_k = y_k \oplus (\bigoplus_{j=1}^{n} x_j a_{jk})$ for each $1 \leq k \leq m$.

Proposition 2 *Every mapping of* $\mathrm{CN}(n, m)$ *can be realized by a quantum circuit consisting of* CN *gates with*

$$O(nm/\gamma + \log(\gamma/n) + \log(\gamma/m))$$

depth and with γ ancillae for $\gamma \geq \min\{n, m\}$.

3 Two Types of Quantum Circuits

Recall that applying a PS gate PS_θ on the j-th qubit realizes the following mapping:

$$|x_1, x_2, \ldots, x_n\rangle \mapsto e^{i\theta(x_j)}|x_1, x_2, \ldots, x_n\rangle.$$

Thus, a quantum circuit, which consists of CN gates and m PS gates $\mathrm{PS}_{\theta_1}, \mathrm{PS}_{\theta_2}, \ldots, \mathrm{PS}_{\theta_m}$, realizes a mapping

$$|x_1, x_2, \ldots, x_n\rangle \mapsto e^{i\sum_{k=1}^{m}\theta_k(y_k)}|z_1, z_2, \ldots, z_n\rangle, \tag{1}$$

such that there exist an $n \times m$ 0-1 matrix $A = [a_{jk}]$ and an $n \times n$ 0-1 matrix $B = [b_{jk}]$ satisfying $y_k = \bigoplus_{j=1}^{n} x_j a_{jk}$ for $1 \leq k \leq m$ and $z_l = \bigoplus_{j=1}^{n} x_j b_{jk}$ for $1 \leq l \leq n$.

Theorem 3 *Quantum circuits consisting* CN *gates and* PS *gates can be parallelized to*

$$O((n^2 + nm)/\gamma + \log(\gamma/n) + \log(\gamma/m))$$

depth by using γ ancillae for $\gamma \geq m$, where m is the number of PS *gates in the quantum circuit.*

Proof The mapping shown in (1) can be realized by using ancillae in four stages. The first stage realizes a mapping

$$|x_1, x_2, \ldots, x_n, 0^m\rangle \mapsto |x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m\rangle.$$

This is mapping of $\mathrm{CN}(n, m)$, and thus from Proposition 2 it can be realized in depth $O(nm/\gamma + \log(\gamma/n) + \log(\gamma/m))$ by using the remaining $\gamma - m$ ancillae. The second stage realizes the mapping

$$|y_1, y_2, \ldots, y_m\rangle \mapsto e^{i\sum_{k=1}^{m}\theta_k(y_k)}|y_1, y_2, \ldots, y_m\rangle$$

by applying the PS gates $\mathrm{PS}_{\theta_1}, \mathrm{PS}_{\theta_2}, \ldots, \mathrm{PS}_{\theta_m}$. Thus it can be done in depth one. The third stage realizes the inverse mapping of one realized in the first stage, i.e.,

$$|x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m\rangle \mapsto |x_1, x_2, \ldots, x_n, 0^m\rangle.$$

Again depth of this stage is $O(nm/\gamma + \log(\gamma/n) + \log(\gamma/m))$. Finally, the fourth stage realizes the mapping

$$|x_1, x_2, \ldots, x_n\rangle \mapsto |z_1, z_2, \ldots, z_n\rangle.$$

From Proposition 1, this stage can be realized in depth $O(n^2/\gamma+\log(\gamma/(n)))$. Therefore, the total depth of these four stages is $O((n^2+nm)/\gamma+\log(\gamma/n)+\log(\gamma/m))$.

■

For quantum circuits consisting of two-input two-output PS gates, we have a efficient realizing.

Lemma 4 *Quantum circuits consisting of two-input two-output* PS *gates with depth d can be parallelized to*

$$O(dn/\gamma+\log(\gamma/n))$$

depth by using γ ancillae for $\gamma \geq n$.

Proof Suppose for $1 \leq k \leq d$ that k-th layer of the quantum circuit realizes a mapping

$$|x_1, x_2, \ldots, x_n\rangle \mapsto e^{i\theta_k(x_1,x_2,\ldots,x_n)}|x_1, x_2, \ldots, x_n\rangle,$$

where $\theta_k : \{0,1\}^n \to [0, 2\pi)$. Thus, the quantum circuit realizes a mapping

$$|x_1, \ldots, x_n\rangle \mapsto e^{i(\theta_1(x_1,\ldots,x_n)+\cdots+\theta_d(x_1,\ldots,x_n))}|x_1, \ldots, x_n\rangle.$$

This mapping can be realized in $\hat{d}+2$ stages. Let $l = \lfloor \gamma/n \rfloor$ and $\hat{d} = \lceil d/l \rceil$. The first stage realizes a mapping

$$|x_1, x_2, \ldots, x_n, 0^{ln}\rangle \mapsto |(x_1, x_2, \ldots, x_n)^{l+1}\rangle.$$

By applying following mapping to each x_j for $1 \leq j \leq n$, this mapping can be realized in depth $O(\log(l+1)) = O(\gamma/n)$. The mapping is

$$|x_j, 0^l\rangle \mapsto |x_j^{l+1}\rangle$$

which can be realized in depth $O(\log(l+1))$.

Then, for $1 \leq \hat{k} \leq \hat{d}$ and $1 \leq l' \leq l$, the $(\hat{k}+1)$-th stage realizes mappings

$$|x_1, \ldots, x_n\rangle \mapsto e^{i(\theta_{(\hat{k}-1)l+1}(x_1,\ldots,x_n)+\cdots+\theta_{\hat{k}l}(x_1,\ldots,x_n))}|x_1, \ldots, x_n\rangle$$

by applying $((\hat{k}-1)l+l')$-th layer to l'-th n-qubit. Thus each of these stages can be realized in depth one. The final stage realizes the inverse mapping of one realized in the first stage, i.e.,

$$|(x_1, x_2, \ldots, x_n)^{l+1}\rangle \mapsto |x_1, x_2, \ldots, x_n, 0^{ln}\rangle.$$

It can be easily verified that the desired mapping, and the total depth is $O(dn/\gamma + \log(\gamma/n))$. ∎

Moore and Nilsson [4] showed that every quantum circuit consisting of CN gates and WH gates can be reconstructed by using an ancilla with state $|1\rangle$ as a quantum circuit with constant number of subcircuits each of which is either a quantum circuit consisting of CN gates, a quantum circuit consisting of WH gates, or a quantum circuit consisting of two-input two-output PS gates with at most $O(n)$ depth. Notice that quantum circuits consisting of WH gates can be realized in at most depth one, since WH WH $= I$. Therefore, from Proposition 1 and Lemma 4, we immediately obtain the following theorem.

Theorem 5 *Quantum circuits consisting of* CN *gates and* WH *gates can be parallelized to*

$$O(n^2/\gamma + \log(\gamma/n))$$

depth by using γ ancillae.

4 Concluding Remarks

We have proposed parallelization methods for the three types of quantum circuits when the number of available ancillae is limited. However, we still do not know any non-trivial lower bound on depth for realizing a desired mapping on the three types of quantum circuits. For more general quantum circuits, parallelization method is still not known. From Barenco *et al* [2], in order to realized universal quantum computation, it is sufficient to consider quantum circuits consisting of CN gates, PS gates, and quantum gates with one-input and one-output, which is specified by

$$\begin{pmatrix} \cos\rho & \sin\rho \\ \sin\rho & -\cos\rho \end{pmatrix}$$

for $0 \leq \rho < 2\pi$, while the WH gate can be specified by this matrix with $\rho = \pi/4$.

References

[1] H. Abe and S.C. Sung, "Parallelizing with Limited Number of Ancillae", JAIST research reports IS-RR-2000-00019, July 4, 2000.

[2] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, "Elementary gates for quantum computation", Phys. Rev **A** (52), pp.3457-3467, 1995.

[3] D. Deutsch, "Quantum computational networks", Proc. Roy. Soc. London Ser. A **425**, pp.73–90, 1989.

[4] C. Moore and M. Nilsson, "Parallel quantum computation and quantum codes", manuscript, 1998 (available at lanl e-print quant-ph/9808027).

[5] A. Yao, "Quantum circuit complexity", in Proc. 34th Annual IEEE Symp. on Foundations of Computer Science, pp.352–361, 1993.